

Streamlining Software Aspects of Certification

SSAC Program Overview

Kelly Hayhurst

SSAC Technical Program Manager
NASA Langley Research Center, Mail Stop 130
Hampton, VA 23681-2199
p: 757-864-6215 f: 757-864-4234
k.j.hayhurst@larc.nasa.gov
<http://shemesh.larc.nasa.gov/ssac/>



Intentions for Workshop III

- Inform you about the SSAC program
 - motivation & background
 - progress to date
 - results of the recent survey on software aspects of certification
- Inform you about the FAA's plan-for-action in response to the SSAC program
- Get your feedback on how well we are doing
- Get your help in defining and implementing improvements to the software approval process



Motivation

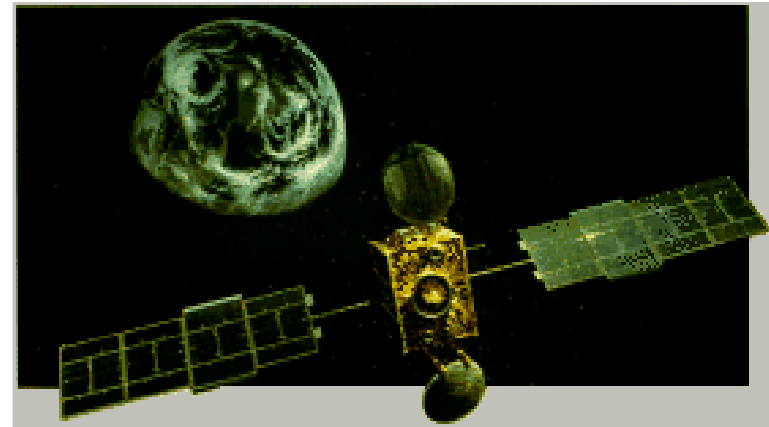
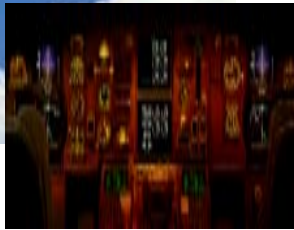
- Modernization of the National Airspace System is inevitable
 - to achieve much needed efficiencies to keep pace with growth and to meet anticipated schedule demands



SSAC Technical Team



Airborne Systems



Satellite Systems



Ground-based Systems



May 25, 1999



"Avionics have never been more clearly at center stage. The benefits of flat-panel and heads-up displays, the precision of GPS positioning, the efficiency of satellite communications, the revolution in automated test equipment, and the flexibility of integrated avionics, to name just a few areas, are transforming aviation almost faster than we can print these words. ... It is no secret that aircraft are becoming ever more dependent on their on-board electronics. The emerging world of CNS and Free Flight promises to accelerate this trend dramatically."

- David Robb, Avionics Magazine, October 1996



Motivation

- Modernization of the National Airspace System (NAS) is inevitable
 - to achieve much needed efficiencies to keep pace with growth and to meet anticipated schedule demands
- Modernization requires many new systems and significant upgrades to existing systems
 - many of these systems have a lot of software
- Software aspects of system development and certification are a big part of project cost and schedule

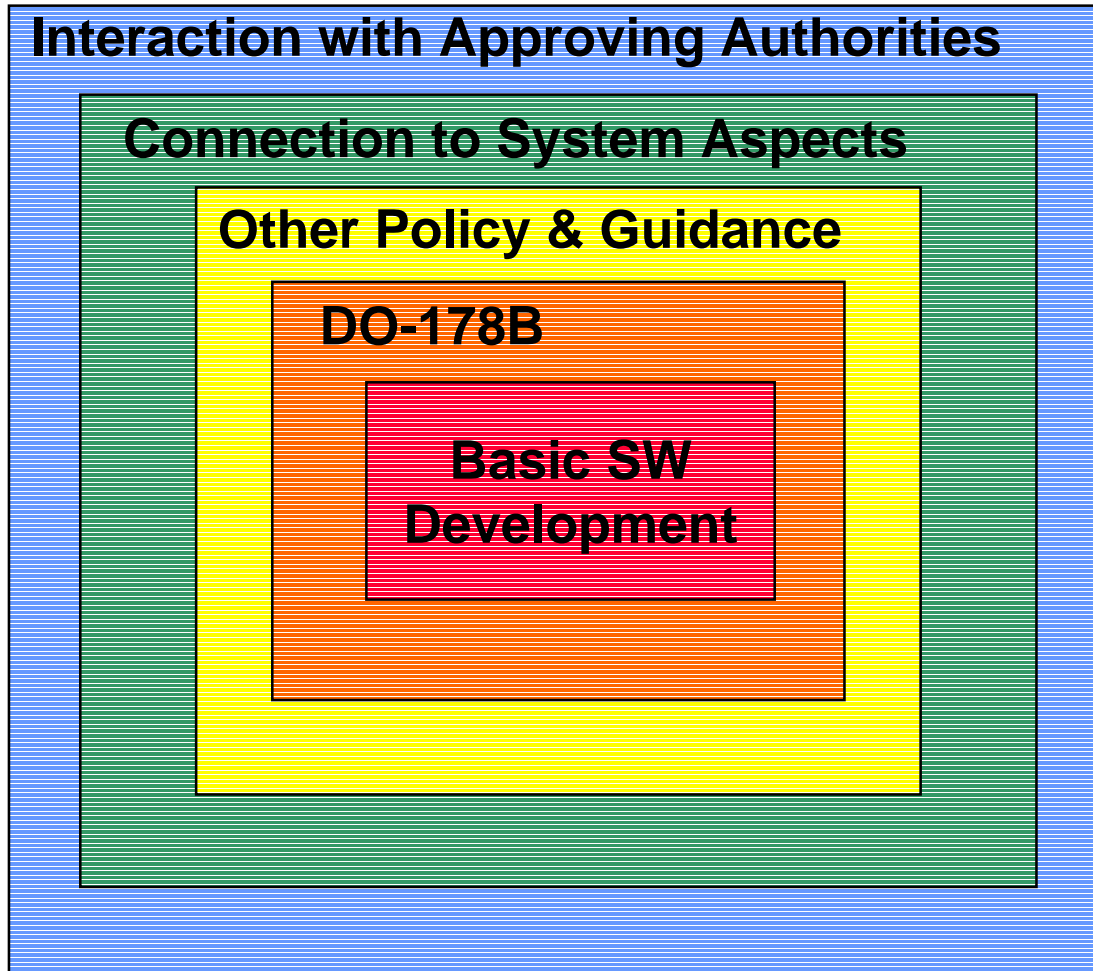


The Cost Connection

- Modernization programs have experienced difficulties (cost & schedule) due to software problems
 - Standard Terminal Automation Replacement System (STARS) and the Wide Area Augmentation System (WAAS)
- Independent studies report inefficiencies that impose additional cost and time burdens
 - 1993 GAO report on Aircraft Certification, RTCA Task Force 4 on Certification, 1999 OIG report on Air Traffic Control Modernization
- Airborne systems developers have complained about cost and time of complying with DO-178B
- Ground-based systems developers are just becoming acquainted with DO-178B and have fears about the cost of compliance



Origins of Cost?



- Need to understand all of the different aspects of software development and approval
 - identify areas for improvement
- Need to determine reasonable basis for making changes to that process



Software Approval within the FAA

- There is no single organization within the FAA that deals with software aspects of approval

Airborne

- Aircraft Certification Service (AIR) deals with certification issues for airborne systems and equipment
- Airborne equipment is certified
 - certification is accomplished in compliance with the Federal Aviation Regulations (FARs)
- For airborne systems, the FAA is only a regulator; i.e., the FAA does not purchase airborne equipment
- DO-178B is the typical means of securing approval

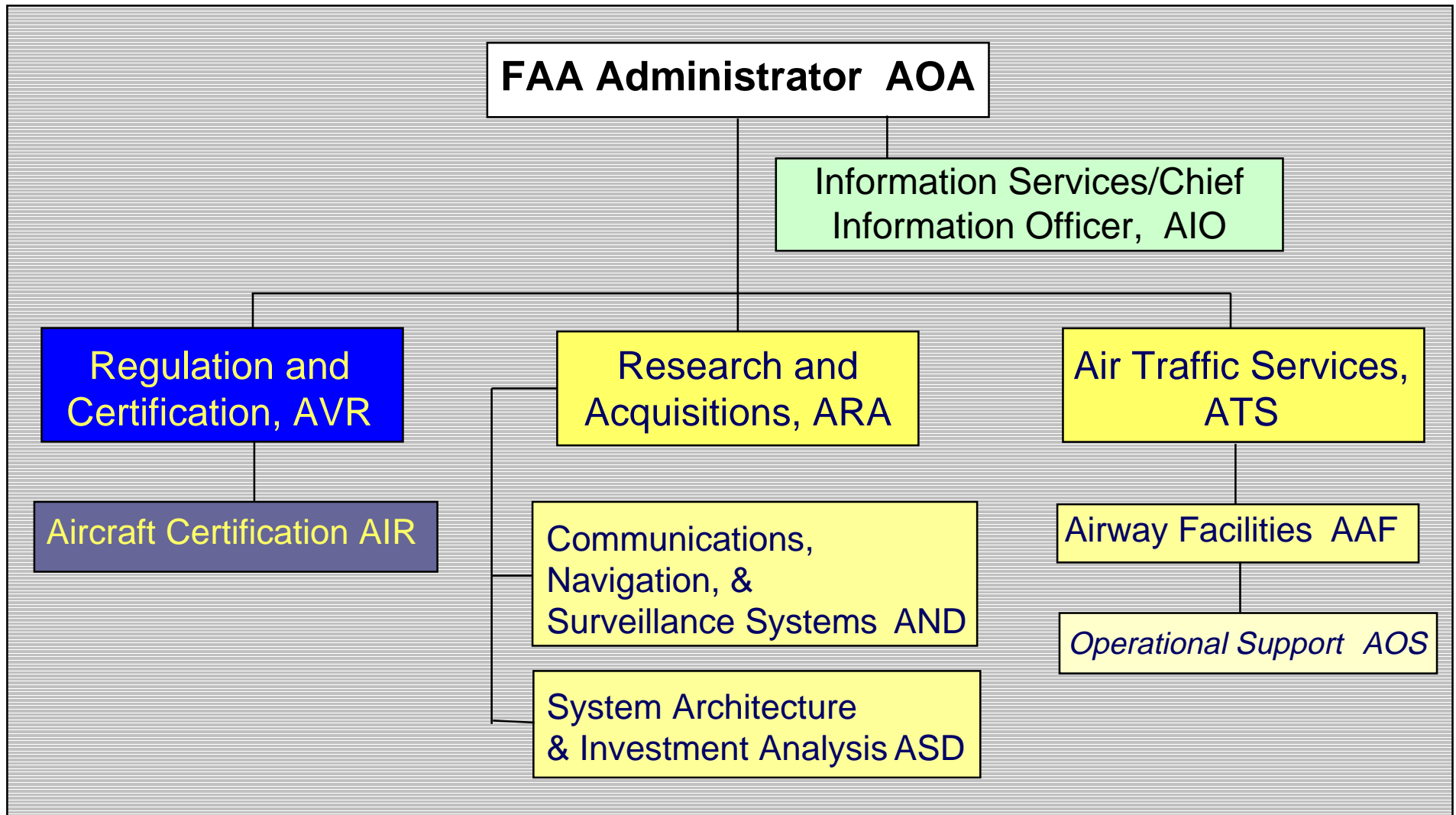
Ground-based

- Research and Acquisitions (ARA) & Air Traffic Services (ATS) are responsible for most ground-based systems and equipment
- Ground-based equipment is "commissioned"
 - approval is determined through FAA Orders and contracts, not FARs
- For ground-based equipment, the FAA is both the acquirer and regulator
- Move to require DO-178B compliance as the means for securing approval



FAA Organization

(relevant to SSAC)





SSAC Program Mission

- In November 1997, the FAA kicked-off the Streamlining Software Aspects of Certification Program

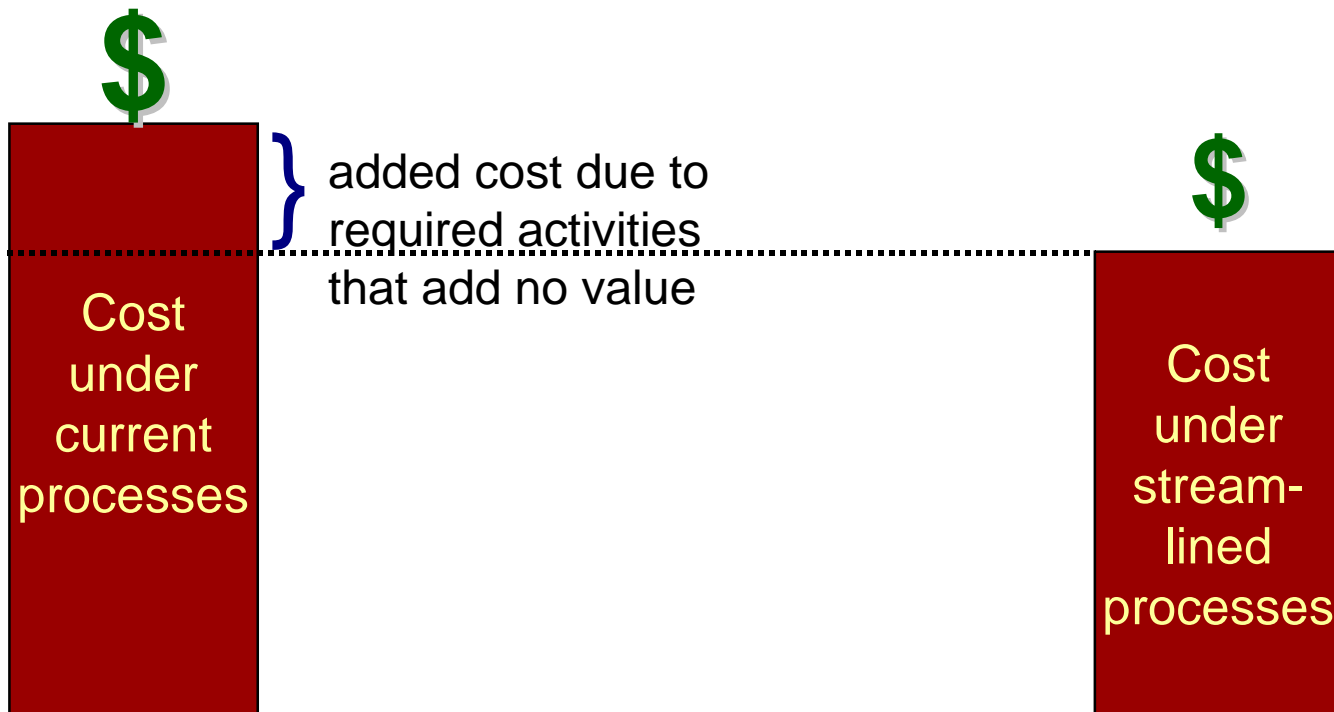
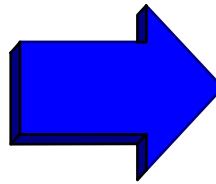
Reduce the cost and time associated with software aspects of certification for both airborne and ground-based systems while maintaining or improving safety

- The FAA commissioned a technical team of experts in software engineering and safety to:
 - provide scientifically/objectively gathered evidence about cost and schedule drivers
 - assess if the cost and time associated with current processes yield the required safety benefit
 - propose and test alternative solutions



Current Situation

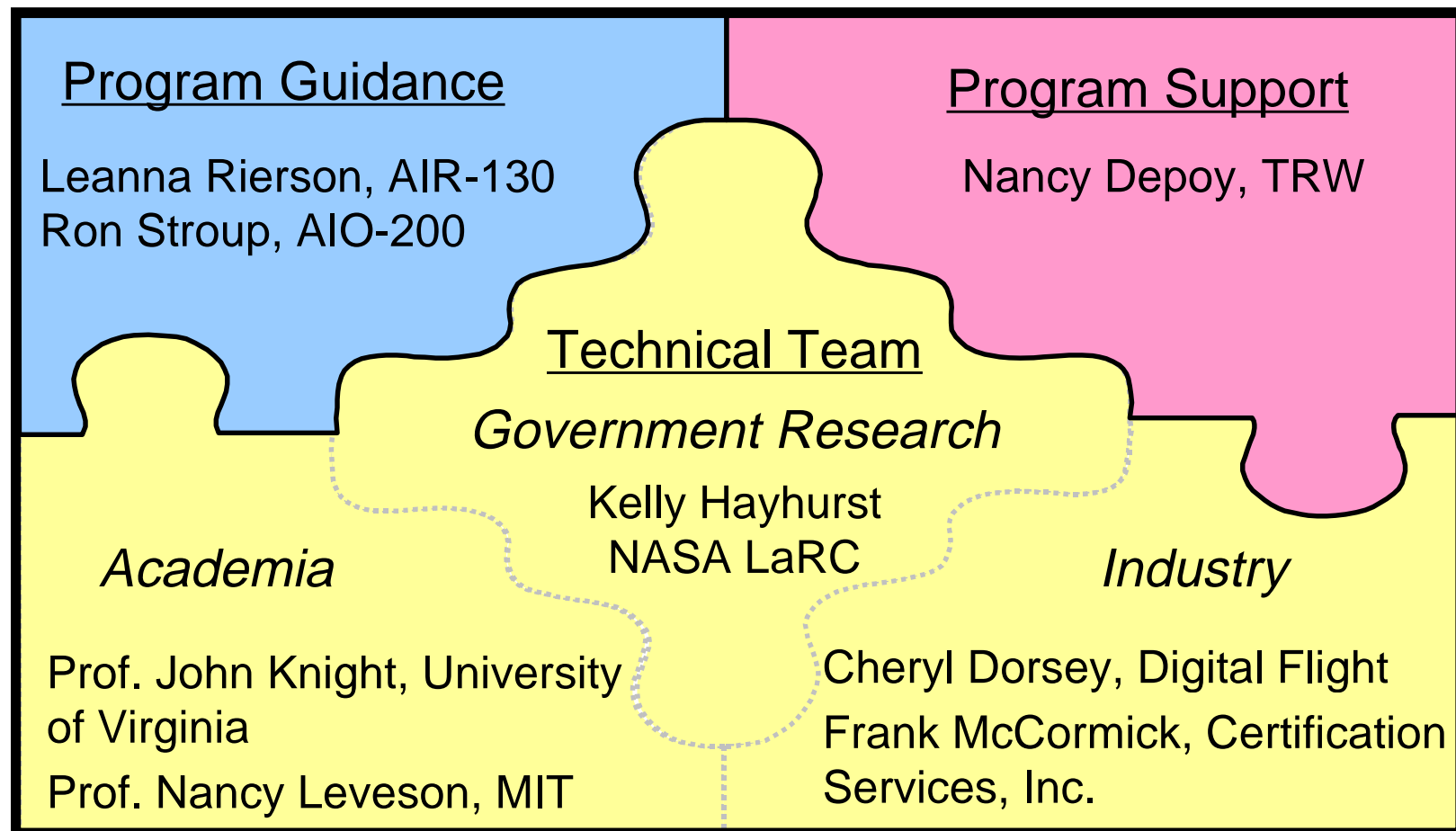
- Situation: Software is perceived to be too expensive and too time consuming.
- Target: Streamlined processes for software development and approval.





Program Organization

- SSAC is a jointly sponsored program: AIO funded & AIR managed





High Level Approach

Let data drive recommendations for streamlining

- Looking at all life cycle costs and schedule issues relevant to software aspects of certification would not be practical
- Focus our effort by understanding the concerns of the FAA and industry
 - making sure to collect sufficient evidence to assess the validity of those concerns
- Work with the FAA and industry to define reasonable data and collection procedures
 - trying to collect data would be infeasible without buy-in from the industry



Program Overview

- **Workshop I, January 1998**
 - industry shared their concerns about software
 - we listened
 - ♦ recorded 200+ potential software issues in Workshop I report
 - ♦ grouped those into 14 issues for further data collection by SSAC



Original 24 Workshop Issues

10 Process Issues:

- Lack of cooperation exists between the FAA and industry.
- Inconsistencies exist among ACOs in interpreting and following policy and guidance.
- Insufficient knowledge of software engineering and related disciplines exists within the FAA.
- Insufficient knowledge of software engineering and related disciplines exists within industry.
- Inadequacies, inconsistencies, and inefficiencies exist in the DER system.
- Insufficient information is available about the certification process.
- Problems exist within the TSO, TC, STC, ATC, and PMA processes.
- Working with non-U. S. certification authorities is difficult.
- Lack of cooperation among companies increases costs.
- Requirements definition is difficult independent of certification.

10 DO-178B Guidance Issues:

- * DO-178B has inadequate and ambiguous guidance for:
 - documentation.
 - planning and configuration management.
 - requirements definition and analysis.
 - partitioning.
 - verification activities.
 - tool qualification.
 - COTS software.
 - reuse of certification data.
 - reuse of legacy systems.
 - non-airborne systems.

4 DO-178B Benefit Issues:

- The extent to which DO-178B provides benefits beyond those that are provided by other industry accepted practices is unclear.
- The effectiveness of some specific activities required by DO-178B is unclear.
- DO-178B inadequately provides for innovation.
- DO-178B inadequately addresses the effect of software on the safety of the overall system.



Program Overview

- **Workshop I**, January 1998
 - industry shared their concerns about software
 - we listened
 - ♦ recorded 200+ potential software issues in Workshop I report
 - ♦ grouped those into 14 issues for further data collection by SSAC
- **Workshop II**, May 1998
 - we jointly prioritized the issues for data collection
 - ♦ high priority issues formed the basis of the SSAC survey
 - started to draft guidance in the areas with clear needs
 - ♦ major/minor software changes, tool qualification, reuse of certification data, and best practices for FAA and industry
- **Survey**, December 1998 - February 1999
 - we assessed extent and significance of the issues



Assessing the Workshop Issues

Provide scientifically/objectively gathered evidence for making intelligent decisions for change

- Determine the extent and significance of the issues for our population **in general**
- Collect data from a large subset of the folks who develop software for airborne and ground-based systems
 - Surveys provide a relatively cheap and effective means for getting a general idea of extent and significance
 - ♦ convenient for sampling a large, geographically-dispersed population
 - ♦ limited time constraints on respondents
 - ♦ can ensure anonymity and confidentiality
 - Surveys cannot provide precise data on cost, but they can help point you in the right direction



SSAC Survey Content

- Interactions with ACOs & other approving authorities
 - inconsistencies
 - lack of cooperation
- Software policy & guidance
- Effectiveness of specific activities in DO-178B
 - independence
 - documentation
 - MCDC
 - quality assurance
 - traceability
 - tool qualification
- Safety
 - connection between DO-178B and safety
- DER system
 - inadequacies, inconsistencies, and inefficiencies



Survey Preparation

- Worked with the Center for Survey Research at the University of Virginia to develop and implement the survey
 - developed 240+ questions
 - reviewed questions for bias and consistency
 - conducted 2 pretests with industry for clarity and completeness
 - ♦ AlliedSignal, Boeing, Rockwell Collins, Honeywell, Litton, and Raytheon participated in the pretests
- Recruited 416 individuals representing 70+ U.S. companies to participate in the survey
 - engineers & managers
 - airborne & ground-based systems developers
 - aircraft & engine manufacturers
 - ♦ all with different levels of experience with DO-178B



Survey Status

- Conducted survey from mid-December through mid-February
- Received final survey data on March 4th
 - tabulated basic frequency distributions & calculated correlation statistics for all survey questions
- Agreed on:
 - survey findings
 - preliminary recommendations
- Prepared draft report on findings and recommendations
 - target date for final survey report is June 30, 1999
- Briefed AVR, AIR, AIO, ARA, and ATS on findings and recommendations
 - expect formal response to recommendations from the FAA by September 30, 1999



Importance of Data

“A little data that is well understood and carefully collected, modeled, and interpreted is better than a vast amount of data without these properties.”

- Manny Lehman, from 201 Principles of Software Development